

CRS Report for Congress

Critical Infrastructures: Background, Policy, and Implementation

Updated January 15, 2008

John D. Motteff
Specialist in Science and Technology Policy
Resources, Science, and Industry Division



Prepared for Members and
Committees of Congress

Report Documentation Page			<i>Form Approved OMB No. 0704-0188</i>	
<p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p>				
1. REPORT DATE 15 JAN 2008	2. REPORT TYPE	3. DATES COVERED 00-00-2008 to 00-00-2008		
4. TITLE AND SUBTITLE Critical Infrastructures: Background, Policy, and Implementation			5a. CONTRACT NUMBER	
			5b. GRANT NUMBER	
			5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)			5d. PROJECT NUMBER	
			5e. TASK NUMBER	
			5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Congressional Research Service, The Library of Congress, 101 Independence Ave, SE, Washington, DC, 20540-7500			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)	
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT				
15. SUBJECT TERMS				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 43
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified	19a. NAME OF RESPONSIBLE PERSON	

Critical Infrastructures: Background, Policy, and Implementation

Summary

The nation's health, wealth, and security rely on the production and distribution of certain goods and services. The array of physical assets, functions, and systems across which these goods and services move are called critical infrastructures (e.g., electricity, the power plants that generate it, and the electric grid upon which it is distributed).

The national security community has been concerned for sometime about the vulnerability of critical infrastructure to both physical and cyber attack. In May 1998, President Clinton released Presidential Decision Directive No. 63. The Directive set up groups within the federal government to develop and implement plans that would protect government-operated infrastructures and called for a dialogue between government and the private sector to develop a National Infrastructure Assurance Plan that would protect all of the nation's critical infrastructures by the year 2003. While the Directive called for both physical and cyber protection from both man-made and natural events, implementation focused on cyber protection against man-made cyber events (i.e., computer hackers). However, given the physical damage caused by the September 11 attacks, physical protections of critical infrastructures has received increased attention.

Following the events of September 11, the Bush Administration released Executive Order 13228, signed October 8, 2001, establishing the Office of Homeland Security. Among its duties, the Office shall "coordinate efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks." In November 2002, Congress passed legislation creating a Department of Homeland Security. Among its responsibilities is overall coordination of critical infrastructure protection activities. In December 2003, the Bush Administration released Homeland Security Presidential Directive 7, reiterating and expanding upon infrastructure protection policy and responsibilities. In June 2006, the Bush Administration released its National Infrastructure Protection Plan. This Plan presents the process by which the Department of Homeland Security intends to identify those specific assets most critical to the United States, across all sectors, based on the risk associated with their loss to attack or natural disaster, and then to prioritize activities aimed at maximizing the reduction of those risks for a given investment.

This report discusses in more detail the evolution of a national critical infrastructure policy and the institutional structures established to implement it. The report highlights five issues of Congressional concern: identifying critical assets; assessing vulnerabilities and risks; allocating resources; information sharing; and, regulation.

Contents

Latest Update Information	1
Introduction	1
Federal Critical Infrastructure Protection Policy: In Brief	2
The President's Commission on Critical Infrastructure Protection	3
Presidential Decision Directive No. 63	4
Restructuring by the Bush Administration	8
Pre-September 11	8
Post-September 11	9
Department of Homeland Security	14
Initial Establishment	14
Second Stage Review Reorganization	15
Post-Katrina Emergency Management Reform Act of 2006	16
Policy Implementation	17
Government — Sector Coordination	17
Appointment of the National Infrastructure Advisory Council	20
Internal Agency Plans	21
National Critical Infrastructure Plan	22
Information Sharing and Analysis Center (ISAC)	24
Identifying Critical Assets, Assessing Vulnerability and Risk, and Prioritizing Protective Measures	25
Issues and Discussion	28
Identifying Critical Assets, Functions, and Systems	28
Assessing Vulnerabilities and Risk	29
Allocating Resources	30
Information Sharing	32
Regulation	34
Appendix	35
Federal Funding for Critical Infrastructure Protection	35
The National Protection and Programs Directorate's FY2008 Budget Request and Appropriations for Infrastructure Protection and Information Security and Other Relevant DHS Budget Activities	36

List of Tables

Table 1. Lead Agencies per PDD-63	5
Table 2. Current Lead Agency Assignments	17

Table 3. Performance Measures for the Infrastructure Protection and Risk Management Program	30
Table A.1. Critical Infrastructure Protection Funding by Department	35
Table A.2 Funding for the Infrastructure Protection and Information Security Program	37

Critical Infrastructures: Background, Policy, and Implementation

Latest Update Information

This update includes the final FY2008 homeland security appropriation provided in the Consolidated Appropriations Act, 2008 (H.R. 2764, P.L. 110-161), passed by the Congress on December 19, 2007, and signed by the President on December 26, 2007. The Appendix on funding has been updated to reflect this final action.

Introduction

Certain socioeconomic activities are vital to the day-to-day functioning and security of the country; for example, transportation of goods and people, communications, banking and finance, and the supply and distribution of electricity and water. Domestic security and our ability to monitor, deter, and respond to outside hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering and command and control of police and military forces. A serious disruption in these activities and capabilities could have a major impact on the country's well-being.¹

These activities and capabilities are supported by an array of physical assets, functions, information, and systems forming what has been called the nation's critical infrastructures. These infrastructures have grown complex and interconnected, meaning that a disruption in one may lead to disruptions in others.²

Disruptions can be caused by any number of factors: poor design, operator error, physical destruction due to natural causes, (earthquakes, lightning strikes, etc.) or physical destruction due to intentional human actions (theft, arson, terrorist attack, etc.). Over the years, operators of these infrastructures have taken measures to guard against, and to quickly respond to, many of these threats, primarily to improve reliability and safety. However, the terrorist attacks of September 11, and the

¹ As a reminder of how dependent society is on its infrastructure, in May 1998, PanAmSat's Galaxy IV satellite's on-board controller malfunctioned, disrupting service to an estimated 80-90% of the nation's pagers, causing problems for hospitals trying to reach doctors on call, emergency workers, and people trying to use their credit cards at gas pumps, to name but a few.

² The electricity blackout in August 2003 in the United States and Canada illustrated the interdependencies between electricity and other elements of the energy market such as oil refining and pipelines, as well as communications, drinking water supplies, etc.

subsequent anthrax attacks, demonstrated the need to reexamine protections in light of the terrorist threat, as part of an overall critical infrastructure protection policy.³

This report provides an historical background and tracks the evolution of such an overall policy and its implementation. However, specific protections associated with individual infrastructures is beyond the scope of this report. For CRS products related to specific infrastructure protection efforts, the reader is encouraged to visit the Terrorism and Homeland Security Current Legislative Issues webpage and look at the Critical Infrastructure Security link.

Federal Critical Infrastructure Protection Policy: In Brief

As discussed further below, a number of federal executive documents and federal legislation lay out a basic policy and strategy for protecting the nation's critical infrastructure. To summarize, it is the policy of the United States to enhance the protection of the nation's critical infrastructure. Critical infrastructure has been defined as those systems and assets, the destruction or incapacity of which would:

- cause catastrophic health effects or mass casualties comparable to those from the use of weapons of mass destruction,
- impair Federal departments and agencies' abilities to perform essential missions or ensure the public's health and safety,
- undermine State and local government capacities to maintain order and deliver minimum essential public services,
- damage the private sector's capability to ensure the orderly functioning of the economy...,
- have a negative effect on the economy through the cascading disruption of other critical infrastructure,
- or undermine the public's morale and confidence in our national economic and political institutions.⁴

The federal government will work with states, localities, and the owners and operators of critical infrastructure (in both the private and public sector) to identify those specific assets and systems that constitute the nation's critical infrastructure. Together, these entities will assess those assets' vulnerabilities to the threats facing

³ Besides loss of life, the terrorist attacks of September 11 disrupted the services of a number of critical infrastructures (including telecommunications, the internet, financial markets, and air transportation). In some cases, protections already in place (like off-site storage of data, mirror capacity, etc.) allowed for relatively quick reconstitution of services. In other cases, service was disrupted for much longer periods of time.

⁴ White House, Homeland Security Presidential Directive Number 7, *Critical Infrastructure Identification, Prioritization, and Protection*. Released December 17, 2003. A more general definition is given in statute (P.L. 107-71, Sec. 1016): "... systems and assets, physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

the nation (natural or manmade, i.e., all hazards), determine the level of risk associated with possible attacks or the impacts of natural events on those assets, and identify and prioritize a set of protection measures that can be taken to reduce those risks. Primary responsibility for protection, response, and recovery lies with the owners and operators.⁵ However, the federal government holds open the possibility of intervening in those areas where owners and operators are unable (or unwilling) to provide what it, the federal government, may assess to be adequate protection or response.⁶

The reader who is not interested in the evolution of this policy and the organizational structures that have evolved to implement it can proceed to the **Policy Implementation** and/or **Issues** sections of this report.

The President's Commission on Critical Infrastructure Protection

This report takes as its starting point the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1996.⁷ Its tasks were to: report to the President the scope and nature of the vulnerabilities and threats to the nation's critical infrastructures (focusing primarily on cyber threats);⁸ recommend a comprehensive national policy and implementation plan for protecting critical infrastructures; determine legal and policy issues raised by proposals to increase protections; and propose statutory and regulatory changes necessary to effect recommendations.

The PCCIP released its report to President Clinton in October 1997.⁹ Examining both the physical and cyber vulnerabilities, the Commission found no immediate crisis threatening the nation's infrastructures. However, it did find reason to take action, especially in the area of cyber security. The rapid growth of a computer-literate population (implying a greater pool of potential hackers), the

⁵ See White House. Office of Homeland Security. *National Strategy for Homeland Security*, p. 33, "Private firms bear primary and substantial responsibility for addressing the public safety risks posed by their industries...."

⁶ Op. cit., p. 33, "The plan will describe how to use all available policy instruments to raise the security of America's critical infrastructure and key assets to a prudent level....In some cases the Department may seek legislation to create incentives for the private sector to adopt security measures.... In some cases, the federal government will need to rely on regulation."

⁷ Executive Order 13010. Critical Infrastructure Protection. Federal Register. Vol. 61, No. 138. July 17, 1996. pp. 3747-3750. Concern about the security of the nation's information infrastructure and the nation's dependence on it preceded the establishment of the Commission.

⁸ Given the growing dependence and interconnectedness of the nation's infrastructure on computer networks, there was concern that computers and computer networks presented a new vulnerability and one that was not receiving adequate attention.

⁹ President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997.

inherent vulnerabilities of common protocols in computer networks, the easy availability of hacker “tools” (available on many websites), and the fact that the basic tools of the hacker (computer, modem, telephone line) are the same essential technologies used by the general population indicated to the Commission that both threat and vulnerability exist.

The Commission generally recommended that greater cooperation and communication between the private sector and government was needed. The private sector owns and operates much of the nation’s critical infrastructure. As seen by the Commission, the government’s primary role (aside from protecting its own infrastructures) is to collect and disseminate the latest information on intrusion techniques, threat analysis, and ways to defend against hackers.

The Commission also proposed a strategy for action:

- facilitate greater cooperation and communication between the private sector and appropriate government agencies by: setting a top level policy-making office in the White House; establishing a council that includes corporate executives, state and local government officials, and cabinet secretaries; and setting up information clearinghouses;
- develop a real-time capability of attack warning;
- establish and promote a comprehensive awareness and education program;
- streamline and clarify elements of the legal structure to support assurance measures (including clearing jurisdictional barriers to pursuing hackers electronically); and,
- expand research and development in technologies and techniques, especially technologies that allow for greater detection of intrusions.

The Commission’s report underwent interagency review to determine how to respond. That review led to a Presidential Decision Directive released in May 1998.

Presidential Decision Directive No. 63

Presidential Decision Directive No. 63 (PDD-63)¹⁰ set as a national goal the ability to protect the nation’s critical infrastructure from intentional attacks (both physical and cyber) by the year 2003. According to the PDD, any interruptions in the ability of these infrastructures to provide their goods and services must be “brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.”¹¹

¹⁰ See *The Clinton’s Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper, May 22, 1998. Available at the Federation of American Scientists website: [<http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>]. This site was last viewed on January 15, 2008.

¹¹ Ibid.

PDD-63 identified the following activities whose critical infrastructures should be protected: information and communications; banking and finance; water supply; aviation, highways, mass transit, pipelines, rail, and waterborne commerce; emergency and law enforcement services; emergency, fire, and continuity of government services; public health services; electric power, oil and gas production, and storage. In addition, the PDD identified four activities where the federal government controls the critical infrastructure: internal security and federal law enforcement; foreign intelligence; foreign affairs; and national defense.

A lead agency was assigned to each of these “sectors” (see **Table 1**). Each lead agency was directed to appoint a **Sector Liaison Official** to interact with appropriate private sector organizations. The private sector was encouraged to select a **Sector Coordinator** to work with the agency’s sector liaison official. Together, the liaison official, sector coordinator, and all affected parties were to contribute to a sectoral security plan which was to be integrated into a **National Infrastructure Assurance Plan**. Each of the activities performed primarily by the federal government also were assigned a lead agency who was to appoint a **Functional Coordinator** to coordinate efforts similar to those made by the Sector Liaisons.

Table 1. Lead Agencies per PDD-63

Department/Agency	Sector/Function
Commerce	Information and Communications
Treasury	Banking and Finance
EPA	Water
Transportation	Transportation
Justice	Emergency Law Enforcement
Federal Emergency Management Agency	Emergency Fire Service
Health and Human Services	Emergency Medicine
Energy	Electric Power, Gas, and Oil
Justice	**Law Enforcement and Internal Security
Director of Central Intelligence	**Intelligence
State	**Foreign Affairs
Defense	**National Defense

** These are the functions identified by PDD-63 as being primarily under federal control.

The PDD also assigned duties to the **National Coordinator** for Security, Infrastructure Protection, and Counter-terrorism.¹² The National Coordinator

¹² The National Coordinator position was created by Presidential Decision Directive 62, “Combating Terrorism.” PDD-62, which was classified, codified and clarified the roles and (continued...)

reported to the President through the Assistant to the President for National Security Affairs.¹³ Among his many duties outlined in PDD-63, the National Coordinator chaired the **Critical Infrastructure Coordination Group**. This Group was the primary interagency working group for developing and implementing policy and for coordinating the federal government's own internal security measures. The Group included high level representatives from the lead agencies (including the Sector Liaisons), the National Economic Council, and all other relevant agencies.

Each federal agency was made responsible for securing its own critical infrastructure and was to designate a Critical Infrastructure Assurance Officer (CIAO) to assume that responsibility. The agency's current Chief Information Officer (CIO) could double in that capacity. In those cases where the CIO and the CIAO were different, the CIO was responsible for assuring the agency's information assets (databases, software, computers), while the CIAO was responsible for any other assets that make up that agency's critical infrastructure. Agencies were given 180 days from the signing of the Directive to develop their plans. Those plans were to be fully implemented within two years and updated every two years.

The PDD set up a **National Infrastructure Assurance Council**. The Council was to be a panel that included private operators of infrastructure assets and officials from state and local government officials and relevant federal agencies. The Council was to meet periodically and provide reports to the President as appropriate. The National Coordinator was to act as the Executive Director of the Council.

The PDD also called for a **National Infrastructure Assurance Plan**. The Plan was to integrate the plans from each of the sectors mentioned above and should consider the following: a vulnerability assessment, including the minimum essential capability required of the sector's infrastructure to meet its purpose; remedial plans to reduce the sector's vulnerability; warning requirements and procedures; response strategies; reconstitution of services; education and awareness programs; research and development needs; intelligence strategies; needs and opportunities for international cooperation; and legislative and budgetary requirements.

The PDD also set up a National Plan Coordination Staff to support the plan's development. Subsequently, the **Critical Infrastructure Assurance Office** (CIAO, not to be confused with the agencies' Critical Infrastructure Assurance Officers) was established to serve this function and was placed in the Department of Commerce's Export Administration. CIAO supported the National Coordinator's efforts to integrate the sectoral plans into a National Plan, supported individual agencies in developing their internal plans, helped coordinate national education and awareness programs, and provided legislative and public affairs support. Coordinating the development of and maintaining the National Plan is now part of the Department of

¹² (...continued)

missions of various agencies engaged in counter-terrorism activities. The Office of the National Coordinator was established to integrate and coordinate these activities. The White House released a fact sheet on PDD-62 on May 22, 1998.

¹³ President Clinton designated Richard Clarke (Special Assistant to the President for Global Affairs, National Security Council) as National Coordinator.

Homeland Security Infrastructure Protection and Information Security (IPIS) program.

Most of the Directive established policy-making and oversight bodies making use of existing agency authorities and expertise. However, the PDD also addressed operational concerns. These dealt primarily with cyber security. The Directive called for a national capability to detect and respond to cyber attacks while they are in progress. Although not specifically identified in the Directive, the Clinton Administration proposed establishing a **Federal Intrusion Detection Network (FIDNET)** that would, together with the **Federal Computer Intrusion Response Capability (FedCIRC)**, established just prior to PDD-63, meet this goal.¹⁴ The Directive explicitly gave the Federal Bureau of Investigation the authority to expand its existing computer crime capabilities into a **National Infrastructure Protection Center (NIPC)**. The Directive called for the NIPC to be the focal point for federal threat assessment, vulnerability analysis, early warning capability, law enforcement investigations, and response coordination. All agencies were required to forward to the NIPC information about threats and actual attacks on their infrastructure as well as attacks made on private sector infrastructures of which they become aware. Presumably, FIDNET¹⁵ and FedCIRC would feed into the NIPC. According to the Directive, the NIPC would be linked electronically to the rest of the federal government and use warning and response expertise located throughout the federal government. The Directive also made the NIPC the conduit for information sharing with the private sector through an equivalent **Information Sharing and Analysis Center(s)** operated by the private sector, which PDD-63 encouraged the private sector to establish. Later, many of these functions were transferred to the Department of Homeland Security. The **U.S. Computer Emergency Response Team (U.S. CERT)** and the **National Operations Center (NOC)**, discussed later in this report, perform similar tasks today.

While the FBI was given the lead, the NIPC also included the Department of Defense, the Intelligence Community, and a representative from all lead agencies. Depending on the level of threat or the character of the intrusion, the NIPC was to have been placed in direct support of either the Department of Defense or the Intelligence Community.

¹⁴ FedCIRC was renamed the Federal Computer Incident Response Center and has since been absorbed into the Department of Homeland Security's National Cyber Security Division.

¹⁵ FIDNET initially generated controversy both inside and outside the government. Privacy concerns, cost and technical feasibility were at issue. By the end of the Clinton Administration, FIDNET as a distributed intrusion detection system feeding into a centralized analysis and warning capability was abandoned. A comparable capability has been developed, called the Einstein Program, that addressed the privacy concerns of FIDNET. Under Einstein, participating agencies retain complete control of network data in strict accordance with Federal laws and policies. Agencies gather and subsequently share security data directly with DHS, based on reporting requirements established by the Office of Management and Budget. In turn, DHS prepares a strategic, cross-agency assessment, which is then shared back with all federal civilian agencies.

Quite independent of PDD-63 in its origin, but clearly complimentary in its purpose, the FBI offers a program called **INFRAGARD** to private sector firms. The program includes an Alert Network. Participants in the program agree to supply the FBI with two reports when they suspect an intrusion of their systems has occurred. One report is “sanitized” of sensitive information and the other provides more detailed description of the intrusion. The FBI will help the participant respond to the intrusion. In addition, all participants are sent periodic updates on what is known about recent intrusion techniques. The FBI has set up local INFRAGARD chapters that can work with each other and regional FBI field offices. In January 2001, the FBI announced it had finished establishing INFRAGARD chapters in each of its 56 field offices. Rather than sector-oriented, INFRAGARD is geographically-oriented. The national program was transferred to the NIPC, before it was absorbed by the Department of Homeland Security. The program is now managed by the FBI’s Cyber Division and is concerned with both cyber and physical threats to critical infrastructure.

It should also be noted that the FBI had, since the 1980s, a program called the **Key Assets Initiative (KAI)**. The objective of the KAI was to develop a database of information on “key assets” within the jurisdiction of each FBI field office, establish lines of communications with asset owners and operators to improve physical and cyber protection, and to coordinate with other federal, state, and local authorities to ensure their involvement in the protection of those assets. The program was initially begun to allow for contingency planning against physical terrorist attacks. According to testimony by a former Director of the NIPC, the program was “reinvigorated” by the NIPC and expanded to include the cyber dimension.¹⁶ The Department of Homeland Security is now responsible for creating a data base of critical assets.

Restructuring by the Bush Administration

Pre-September 11

As part of its overall redesign of White House organization and assignment of responsibilities, the in-coming Bush Administration spent the first eight months reviewing its options for coordinating and overseeing critical infrastructure protection. During this time, the Bush Administration continued to support the activities begun by the Clinton Administration.

The Bush Administration review was influenced by three parallel debates. First, the National Security Council (NSC) underwent a major streamlining. All groups within the Council established during previous Administrations were abolished. Their responsibilities and functions were consolidated into 17 Policy Coordination Committees (PCCs). The activities associated with critical infrastructure protection were assumed by the Counter-Terrorism and National Preparedness PCC. At the

¹⁶ Testimony by Michael Vatis before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism. October 6, 1999. This effort was transferred to the Department of Homeland Security.

time, whether, or to what extent, the NSC should remain the focal point for coordinating critical infrastructure protection (i.e., the National Coordinator came from the NSC) was unclear. Richard Clarke, himself, wrote a memorandum to the incoming Bush Administration advocating that the function should be transferred directly to the White House.¹⁷

Second, there was a continuing debate about the merits of establishing a government-wide Chief Information Officer (CIO), whose responsibilities would include protection of all federal non-national security-related computer systems and coordination with the private sector on the protection of privately owned computer systems. Shortly after assuming office, the Bush Administration announced its desire not to create a separate federal CIO position, but to recruit a Deputy Director of the Office of Management and Budget that would assume an oversight role of agency CIOs. One of the reasons cited for this was a desire to keep agencies responsible for their own computer security.¹⁸

Third, there was the continuing debate about how best to defend the country against terrorism, in general. The U.S. Commission on National Security/21st Century (the Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation built upon the current Federal Emergency Management Agency (FEMA) by adding to it the Coast Guard, the Border Patrol, Customs Service, and other agencies. The Commission recommended that the new organization include a directorate responsible for critical infrastructure protection. While both the Clinton and Bush Administration remained cool to this idea, bills were introduced in Congress to establish such an agency. As discussed below, the Bush Administration changed its position in June 2002, and proposed a new department along the lines of that proposed by the Hart/Rudman Commission and Congress.

Post-September 11

Soon after the September 11 terrorist attacks, President Bush signed two Executive Orders relevant to critical infrastructure protection. These have since been amended to reflect changes brought about by the establishment of the Department of Homeland Security (see below). The following is a brief discussion of the original E.O.s and how they have changed.

E.O. 13228, signed October 8, 2001 established the **Office of Homeland Security**, headed by the **Assistant to the President for Homeland Security**.¹⁹ Its mission is to “develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats and attacks.”

¹⁷ Senior NSC Official Pitches Cyber-Security Czar Concept in Memo to Rice. *Inside the Pentagon*. January 11, 2001. p. 2-3.

¹⁸ For a discussion of the debate surrounding this issue at the time, see CRS Report RL30914, *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffery Seifert.

¹⁹ President Bush selected Tom Ridge to head the new Office.

Among its functions is the coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. This includes strengthening measures for protecting energy production, transmission, and distribution; telecommunications; public and privately owned information systems; transportation systems; and, the provision of food and water for human use. Another function of the Office is to coordinate efforts to ensure rapid restoration of these critical infrastructures after a disruption by a terrorist threat or attack.

The EO also established the **Homeland Security Council**. The Council is made up of the President, Vice-President, Secretaries of Treasury, Defense, Health and Human Services, and Transportation, the Attorney General, the Directors of FEMA, FBI, and CIA and the Assistant to the President for Homeland Security. The EO was later amended to add the Secretary of Homeland Security. Other White House and departmental officials can be invited to attend Council meetings.²⁰ The Council advises and assists the President with respect to all aspects of homeland security. The agenda for those meetings shall be set by the Assistant to President for Homeland Security, at the direction of the President. The Assistant is also the official recorder of Council actions and Presidential decisions.

In January and February 2003, this E.O. was amended (by Executive Orders 13284 and 13286, respectively). The Office of Homeland Security, the Assistant to the President, and the Homeland Security Council were all retained. However, the Secretary of Homeland Security was added to the Council. The duties of the Assistant to the President for Homeland Security remain the same, recognizing the statutory duties assigned to the Secretary of Homeland Security as a result of the Homeland Security Act of 2002 (see below).

The second Executive Order (E.O. 13231) signed October 16, 2001, stated that it is U.S. policy “to protect against the disruption of the operation of information systems for critical infrastructure...and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible.”²¹ This Order also established the **President’s Critical Infrastructure Protection Board**. The Board, consisting of federal officials, was authorized to “recommend policies and coordinate programs for protecting information systems for critical infrastructure...” The Board also was directed to propose a National Plan on issues within its purview on a periodic basis, and, in coordination with the Office of Homeland Security, review and make recommendations on that part of agency budgets that fall within the purview of the Board.

The Board was chaired by a **Special Advisor to the President for Cyberspace Security**.²² The Special Advisor reported to both the Assistant to the President for

²⁰ For more information on the structure of the Homeland Security Council and the Office of Homeland Security, see CRS Report RL31148, *Homeland Security: The Presidential Coordination Office*, by Harold Relyea.

²¹ Executive Order 13231 — Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 86. No. 202. October 18, 2001.

²² President Bush designated Richard Clarke.

National Security and the Assistant to the President for Homeland Security. Besides presiding over Board meetings, the Special Advisor, in consultation with the Board, was to propose policies and programs to appropriate officials to ensure protection of the nation's information infrastructure and to coordinate with the Director of OMB on issues relating to budgets and the security of computer networks.

The Order also established the **National Infrastructure Advisory Council**. The Council is to provide advice to the President on the security of information systems for critical infrastructure. The Council's functions include enhancing public-private partnerships, monitoring the development of ISACs, and encouraging the private sector to perform periodic vulnerability assessments of critical information and telecommunication systems.

Subsequent amendments to this E.O. (by E.O. 13286) abolished the President's Board and the position of Special Advisor. The Advisory Council was retained, but now reports to the President through the Secretary of Homeland Security.

In July 2002, the Office of Homeland Security released a *National Strategy for Homeland Security*. The Strategy covered all government efforts to protect the nation against terrorist attacks of all kinds. It identified protecting the nation's critical infrastructures and key assets (a new term, different as implied above by the FBI's key asset program) as one of six critical mission areas. The Strategy expanded upon the list of sectors considered to possess critical infrastructure to include public health, the chemical industry and hazardous materials, postal and shipping, the defense industrial base, and agriculture and food. The *Strategy* also added continuity of government and continuity of operations to the list, although it is difficult to see how the latter would be a considered sector. It also combined emergency fire service, emergency law enforcement, and emergency medicine as emergency services. And, it dropped those functions that primarily belonged to the federal governments (e.g. defense, intelligence, law enforcement). It also reassigned some of the sectors to different agencies, including making the then proposed Department of Homeland Security lead agency for a number of sectors — postal and shipping services, and the defense industrial base. It also introduced a new class of assets, called key assets, which was defined as potential targets whose destruction may not endanger vital systems, but could create a local disaster or profoundly affect national morale. Such assets were defined later to include national monuments and other historic attractions, dams, nuclear facilities, and large commercial centers, including office buildings and sport stadiums, where large numbers of people congregate to conduct business, personal transactions, or enjoy recreational activities.²³

The Strategy reiterated many of the same policy-related activities as mentioned above: working with the private sector and other non-federal entities, naming those agencies that should act as liaison with the private sector, assessing vulnerabilities, and developing a national plan to deal with those vulnerabilities. The Strategy also mentioned the need to set priorities, acknowledging that not all assets are equally critical, and that the costs associated with protecting assets must be balanced against

²³ The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003. p. 71.

the benefits of increased security according to the threat. The Strategy did not create any new organizations, but assumed that a Department of Homeland Security would be established (see below).

On December 17, 2003, the Bush Administration released **Homeland Security Presidential Directive 7 (HSPD-7)**. HSPD essentially updated the policy of the United States and the roles and responsibilities of various agencies in regard to critical infrastructure protection as outlined in previous documents, national strategies, and the Homeland Security Act of 2002 (see below). For example, the Directive reiterated the Secretary of Homeland Security's role in coordinating the overall national effort to protect critical infrastructure. It also reiterated the role of Sector-Specific Agencies (i.e., Lead Agencies)²⁴ to work with their sectors to identify, prioritize, and coordinate protective measures. The Directive captured the expanded set of critical infrastructures and key assets and Sector-Specific Agencies assignments made in the *National Strategy for Homeland Security*. The Directive also reiterated the relationship between the Department of Homeland Security and other agencies in certain areas. For example, while the Department of Homeland Security will maintain a cyber security unit, the Directive stated that the Director of the Office of Management remains responsible for overseeing government-wide information security programs and for ensuring the operation of a federal cyber incident response center within the Department of Homeland Security. Also, while the Department of Homeland Security is responsible for transportation security, including airline security, the Department of Transportation remains responsible for control of the national air space system.

The only organizational change made by the Directive was the establishment of the **Critical Infrastructure Protection Policy Coordinating Committee** which will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure security.

The Directive made a few other noticeable changes or additions. For example, the Department of Homeland Security was assigned as Lead Agency for the chemical and hazardous materials sector (it had been the Environmental Protection Agency). The Directive required Lead Agencies to report annually to the Secretary of Homeland Security on their efforts in working with the private sector. The Directive also reiterated that all federal agencies must develop plans to protect their own critical infrastructure and submit those plans for approval to the Director of the Office of Management and Budget by July 2004.

The Bush Administration policy and approach regarding critical infrastructure protection can be described as an evolutionary expansion of the policies and approaches laid out in PDD-63. The fundamental policy statements are essentially the same: the protection of infrastructures critical to the people, economy, essential government services, and national security. National morale was added to that list. Also, the stated goal of the government's efforts is to ensure that any disruption of the services provided by these infrastructures be infrequent, of minimal duration, and

²⁴ This report will continue to use the term "Lead Agency" to refer to the agency assigned to work with a specific sector.

manageable. The infrastructures identified as critical were essentially the same (although expanded and with an emphasis placed on targets that would result in large numbers of casualties). Finally, the primary effort is directed at working collaboratively and voluntarily with the private sector owners and operators of critical infrastructure to identify critical assets and provide appropriate protection.

Organizationally, there remains an interagency group for coordinating policy across departments and for informing the White House (Homeland Security Council, supported by the Critical Infrastructure Protection Coordinating Committee). Certain agencies have been assigned certain sectors with which to work. Sectors are asked to organize themselves to assist in coordination of effort and information sharing. A Council made up of private sector executives, academics, and State and local officials was established to advise the President. Certain operational units (e.g., the Critical Infrastructure Assurance Office (CIAO) and elements of the National Infrastructure Protection Center (at the FBI)) were initially left in place, though later moved to and restructured within the Department of Homeland Security (DHS), where, now, the Undersecretary for National Protection and Programs is responsible for coordinating the implementation of policies and programs (see below). However, DHS takes a much more active role in identifying critical assets, assessing vulnerabilities, and recommending and supporting protective measures than did these earlier operational units. Also, the manpower and resources devoted to these activities have greatly increased.

One major difference between PDD-63 and the current Administration's efforts is a shift in focus. PDD-63 focused on cybersecurity. While the post-September 11 effort is still concerned with cybersecurity, its focus on physical threats, especially those that might cause mass casualties, is greater than the pre-September 11 effort. This led to some debate and organizational instability initially. The early executive orders discussed above segregated cyber security from the physical security mission with the formation of the Office of Homeland Security and the President's Critical Infrastructure Protection Board. Dissolution of the Board and the subsequent establishment of the Critical Infrastructure Protection Policy Coordinating Committee, responsible for advising the Homeland Security Council on both physical and cyber security issues, would appear to reunite these two concerns within a single White House group.²⁵

²⁵ Computer security advocates have sought to highlight cyber security issues by maintaining a separate organization high within the bureaucracy. There now exists both an Assistant Secretary for Cyber Security and Telecommunications and an Assistant Secretary for Infrastructure Protection, both reporting to the Undersecretary for National Protection and Programs. While the latter is concerned with both physical and cyber security issues, the former is focused on cyber security issues.

Department of Homeland Security

Initial Establishment

In November 2002, Congress passed the Homeland Security Act (P.L. 107-296), establishing a **Department of Homeland Security (DHS)**. The act assigned to the new Department the mission of preventing terrorist attacks, reducing the vulnerability of the nation to such attacks, and responding rapidly should such an attack occur. The act essentially consolidated within one department a number of agencies that had, as part of their missions, homeland security-like functions (e.g., Border Patrol, Customs, Transportation Security Administration). The following discussion focuses on those provisions relating to critical infrastructure protection.

In regard to critical infrastructure protection the act transferred the following agencies and offices to the new department: the NIPC (except for the Computer Investigations and Operations Section), CIAO, FedCIRC, the **National Simulation and Analysis Center (NISAC)**,²⁶ other energy security and assurance activities within DOE, and the **National Communication System (NCS)**.²⁷ These agencies and offices were integrated within the **Directorate of Information Analysis and Infrastructure Protection (IA/IP)** (one of four operational Directorates established by the act).²⁸ Notably, the Transportation Security Administration (TSA), which is responsible for securing all modes of the nation's transportation system, was not made part of this Directorate (it was placed within the Border and Transportation Security Directorate); nor was the Coast Guard, which is responsible for port security. The act assigned the rank of Undersecretary to the head of each Directorate. Furthermore, the act designated that within the Directorate of Information Analysis and Infrastructure Protection, there were to be both an Assistant Secretary for Information Analysis, and an **Assistant Secretary for Infrastructure Protection**.

²⁶ The NISAC was established in the USA PATRIOT Act (P.L. 107-56), Section 1062. The Center builds upon expertise at Sandia National Laboratory and Los Alamos National Laboratory in modeling and simulating infrastructures and the interdependencies between them.

²⁷ The NCS is not a single communication system but more a capability that ensures that disparate government agencies can communicate with each other in times of emergencies. To make sure this capability exists and to assure that it is available when needed, an interagency group meets regularly to discuss issues and solve problems. The NCS was initially established in 1963 by the Kennedy Administration to ensure communications between military, diplomatic, intelligence, and civilian leaders, following the Cuban Missile Crisis. Those activities were expanded by the Reagan Administration to include emergency preparedness and response, including natural disaster response. The current interagency group includes 23 departments and agencies. The private sector, which own a significant share of the assets needed to ensure the necessary connectivity, is involved through the **National Security Telecommunication Advisory Committee (NSTAC)**. The National Coordinating Center, mentioned later in this report, and which serves as the telecommunications ISAC, is an operational entity within the NCS.

²⁸ The other operational directorates included **Science and Technology**, **Border and Transportation Security** and **Emergency Preparedness and Response**.

Among the responsibilities assigned the IA/IP Directorate were:

- to access, receive, analyze, and integrate information from a variety of sources in order to identify and assess the nature and scope of the terrorist threat;
- to carry out comprehensive **assessments of the vulnerabilities** of key resources and critical infrastructure of the United States, including **risk assessments** to determine risks posed by particular types of attacks;
- to integrate relevant information, analyses, and vulnerability assessments in order to **identify priorities for protective and support measures**;
- to develop a comprehensive national plan for securing key resources and critical infrastructures;
- to administer the Homeland Security Advisory System;
- to work with the intelligence community to establish collection priorities; and,
- to establish a secure communication system for receiving and disseminating information.

In addition, the act provided a number of protections for certain information (defined as critical infrastructure information) that non-federal entities, especially private firms or ISACs formed by the private sector, voluntarily provide the Department. Those protections included exempting it from the Freedom of Information Act, precluding the information from being used in any civil action, exempting it from any agency rules regarding ex parte communication, and exempting it from requirements of the Federal Advisory Committee Act.

The act basically built upon existing policy and activities. Many of the policies, objectives, missions, and responsibilities complement those already established (e.g., vulnerability assessments, national planning, communication between government and private sector, and improving protections).

Second Stage Review Reorganization

Secretary Chertoff (the second Secretary of Homeland Security), as one of his Second Stage Review recommendations, proposed restructuring the IA/IP Directorate and renaming it the **Directorate of Preparedness**. The IA function was merged into a new **Office of Intelligence and Analysis**. The IP function, with the same missions as outlined in the Homeland Security Act, remained, but was joined by other existing and new entities. The renamed Directorate included elements from Office of State and Local Government Coordination and Preparedness, including its principal grant-making functions and some of the preparedness functions of the Federal Emergency Management Agency (FEMA). A new position of Chief Medical Officer was created within the Directorate and the U.S. Fire Administration and the Office of National Capital Region Coordination were transferred into the Directorate. In addition, the restructuring called for an **Assistant Secretary for Cyber Security and Telecommunications** (a position long sought by many within the cyber security community) and an Assistant Secretary for Infrastructure Protection.

According to the DHS press release, the mission of the restructured Directorate was to “facilitate grants and over see nationwide preparedness efforts supporting first responder training, citizen awareness, public health, infrastructure and cyber security, and [to] ensure proper steps are taken to protect high-risk targets.”

Other recommendations resulting from the review that may impact infrastructure protection included moving the Homeland Security Operations Center, now called the National Operations Center, out of the old IA/IP Directorate and placing it within a new Office of Operations Coordination; and, a new Directorate of Policy, which is described as serving as the primary Department-wide coordinator of policies, regulations, and other initiatives. The conference committee report on the Department’s FY2006 appropriations (H.Rept. 109-241) approved these changes.²⁹

Post-Katrina Emergency Management Reform Act of 2006

The Post-Katrina Emergency Management Reform Act of 2006 (referred hereon as the Post-Katrina Act) was passed as Title VI of the Department of Homeland Security Appropriations Act, 2007 (P.L. 109-295). The Post-Katrina Act reunited the Department’s preparedness activities with its response and recovery activities within a restructured Federal Emergency Management Agency (FEMA). The Post-Katrina Act explicitly preserved the restructured FEMA as a distinct entity within the Department. The Post-Katrina Act also transferred the Preparedness Directorate’s Office of Grants and Training to the restructured FEMA. The Post-Katrina Act left the remaining activities, including those associated with the Office of the Chief Medical Officer and the critical infrastructure protection activities associated with the Assistant Secretary of Infrastructure Protection and the Assistant Secretary for Cyber Security and Telecommunications, in the Preparedness Directorate. The Post-Katrina Act also established the **Office of Emergency Communications** and required that it report to the Assistant Secretary for Cyber Security and Telecommunications. The Office of Emergency Communications has within its responsibilities a number of activities associated with assisting interoperable communications among first responders.

On January 18, 2007, Secretary Chertoff submitted to Congress a description of the Department’s reorganization pursuant to the Post-Katrina Act, and additional changes made pursuant to the Secretary’s authority provided in the Homeland Security Act (P.L. 107-296, Section 872). Under this latter authority, the Secretary renamed the Preparedness Directorate the **National Protection and Programs Directorate** (NPPD), still to be headed by someone of Undersecretary rank. The NPPD includes the Office of the Undersecretary, the Office of Cybersecurity and Communications (including the new Office of Emergency Communications), the Office of Infrastructure Protection, the Office of Risk Management and Analysis (formerly a division of the Office of Infrastructure Protection), and the Office of

²⁹ See report language in H.Rept. 109-241, accompanying H.R. 2360, September 2005, p. 29.

Intergovernmental Programs. In addition, the Secretary moved the U.S.-VISIT program into the NPPD.³⁰

The Secretary also, pursuant to his Section 872 authority, transferred the Chief Medical Officer to head a new Office of Health Affairs. This new Office reports to the Secretary through the Deputy Secretary. This reorganization consolidated activities associated with the Department's bio-defense efforts, including the transfer of the Biosurveillance program, formerly part of the Infrastructure Protection and Information Security (IPIS) Program (see Appendix). Except for the transfer of the Biosurveillance program, the IPIS program, which represents the core of the Department's effort to coordinate the nation's critical infrastructure protection activities, remains in the National Protection and Programs Directorate.

Policy Implementation

Government — Sector Coordination

The number and breakdown of sectors and lead, or sector specific agencies, have expanded and changed since the assignments made by PDD-63 (and noted in **Table 1** of this report). As mentioned above, the Bush Administration has expanded the number of sectors considered to possess critical infrastructure and made some changes in assignments. **Table 2**, below, shows the current list of sectors and their lead agencies, as defined in the National Infrastructure Protection Plan released June 2006.

Table 2. Current Lead Agency Assignments

Department/Agency	Sector/Subsector
Agriculture	Agriculture
	Food
Agriculture	Meat/Poultry
Health and Human Services	All other
Treasury	Banking and Finance
EPA	Drinking Water and Water Treatment Systems
Health and Human Services	Public Health and Healthcare
Defense	Defense Industrial Base
Interior	National Monuments and Icons
Energy	Energy ^a
Homeland Security	Transportation Systems ^b

³⁰ U.S.-VISIT is the Department's effort to verify the identity of people entering and exiting the United States.

Department/Agency	Sector/Subsector
Homeland Security	Postal and Shipping
Homeland Security	Information Technology
Homeland Security	Communications
Homeland Security	Commercial Nuclear Reactors, Materials, and Waste
Homeland Security	Chemical
Homeland Security	Emergency Services
Homeland Security	Dams
Homeland Security	Commercial Facilities
Homeland Security	Government Facilities

- a. While noted here as a single sector, in practice it is represented by two relatively separate sectors: electric power (except for nuclear power facilities); and the production, refining, and some distribution of oil and gas. The Department of Energy is the lead agency for both. However, the Department of Homeland Security (through the Transportation Security Administration) is the lead agency for the distribution of oil and gas via pipelines. Nuclear power is considered its own sector.
- b. While noted here as a single sector, Transportation includes all modes of transportation: rail, mass transit (rail and bus), air, maritime, highways, pipelines, etc. The Transportation Security Administration within the Department of Homeland Security, in collaboration with the Department of Transportation, is the lead agency for all but the maritime subsector, for which the Coast Guard, also within the Department of Homeland Security, acts as lead agency.

PDD-63 called for the selection, by each Lead Agency, of a Sector Liaison Official (representing the Lead Agency) and a Sector Coordinator (representing the owners/operators of each sector). While most agencies quickly identified their Sector Liaison Official, it took more time to identify Sector Coordinators. Different sectors present different challenges for coordination. Some sectors are more diverse than others (e.g., transportation includes rail, air, waterways, and highways; information and communications include computers, software, wire and wireless communications) and raise the issue of how to have all the relevant players represented. Other sectors are fragmented, consisting of small or local entities. Some sectors, such as banking, telecommunications, and energy have more experience than others in working with the federal government and/or working collectively to assure the performance of their systems.

In addition to such structural issues are ones related to competition. Inherent in the exercise is asking competitors to cooperate. In some cases it is asking competing industries to cooperate. This cooperation not only raises issues of trust among firms, but also concerns regarding anti-trust rules.

Over time, Sector Coordinators were selected for most of the sectors identified under PDD-63. Typically, a representative from a relevant trade organizations was chosen to act as sector coordinator. For example, the Environmental Protection Agency selected the Executive Director of the Association of Metropolitan Water Agencies to act as Sector Coordinator for the water sector. In the case of the law

enforcement sector (no longer identified as a separate sector), the National Infrastructure Protection Center helped create a Emergency Law Enforcement Services Forum, consisting of senior state, local, and non-FBI law enforcement officials. In the case of banking and finance, the Sector Coordinator was chosen from a major banking/finance institution, who doubled as the Chairperson of the Financial Services Sector Coordinating Council, an organization specifically set up by the industry to coordinate critical infrastructure protection activities with the federal government.

In December 1999, a number of the sectors formed a **Partnership for Critical Infrastructure Security** to share information and strategies and to identify interdependencies across sectoral lines. The Partnership was a private sector initiative. The federal government was not officially part of the Partnership, but the Department of Homeland Security (and CIAO before that) acted as a liaison and provided administrative support for meetings. Sector Liaisons from lead agencies were considered ex officio members. The Partnership helped coordinate its members input to a number of the national strategies released to date and were to provide input into the National Plan called for in PDD-63.

While initially working with this organizational structure, the Bush Administration promoted a new Critical Infrastructure Protection Partnership Model. Resembling the Financial Services Sector Coordinating Council approach, this newer Model expanded the sector liaison and sector coordinator model of PDD-63 into **Government Coordinating Councils** and **Sector Coordinating Councils** for each sector. The primary objective was to expand both owner/operator and government representation within all sectors. Now, for example, the Water Sector Coordinating Council consists of two owner/operator representatives, along with one non-voting association staff, from each of the following participating organizations: the Association of Metropolitan Water Agencies, the American Water Works Association, the American Water Works Association Research Foundation, the National Association of Clean Water Agencies, the National Association of Water Companies, the National Rural Water Association, the Water Environment Federation, and the Water Environment Research Foundation. The Water Government Coordinating Council is chaired by the Environmental Protection Agency, the Lead Agency, but also includes the Department of Homeland Security, the Food and Drug Administration, the Department of Interior, and the Center for Disease Control. Government Coordinating Councils can also include state, local, and tribal government entities. The Sector Coordinating Councils are to establish their own organizational structures and leadership and act independently from the federal government. Also, under this model, the Partnership for Critical Infrastructure Security has been designated the **Private Sector Cross-Sector Council**. The Sector Coordinating Councils are to provide input into both the National Infrastructure Protection Plan and the individual Sector Specific Plans (see below). Many of the issues governing the progress made in identifying and working with the sector coordinators model of PDD-63 continue with the sector coordinating councils.³¹

³¹ See U.S. Congress. General Accountability Office. *Critical Infrastructure Protection:* (continued...)

In March 2006, the Department of Homeland Security used its authority under the Homeland Security Act (P.L. 107-296, Section 871) — to form advisory committees that are exempt from the Federal Advisory Committee Act (P.L. 92-463) — to establish the **Critical Infrastructure Partnership Advisory Council (CIPAC)**.³² The Federal Advisory Committee Act requires advisory committees generally to meet in open session and make written materials available to the public. The purpose of waiving this act for the CIPAC is to facilitate more open discussion between the sector coordinating councils and the government coordinating councils (if not with the public). DHS acts as the Executive Secretariat. Members include owner/operators that are members of their respective sector coordinating councils or belong to an association that is a member of the coordinating council. Members also include federal, state, local, and tribal government entities that belong to their respective government coordinating councils. While the CIPAC is exempt from the Federal Advisory Committee Act, DHS stated in its public notice that it will make meeting dates and appropriate agendas available. There is a CIPAC webpage on the DHS website.³³

Appointment of the National Infrastructure Advisory Council

The Clinton Administration released an Executive Order (13130) in July, 1999, formally establishing the National Infrastructure Assurance Council. Just prior to leaving office, President Clinton put forward the names of 18 appointees.³⁴ The Order was rescinded by the Bush Administration before the Council could meet. In Executive Order 13231,³⁵ President Bush established a National Infrastructure Advisory Council (with the same acronym, NIAC) whose functions are similar to those of the Clinton Council. On September 18, 2002, President Bush announced his appointment of 24 individuals to serve on Council.³⁶ The E.O. amending 13231 makes some minor modifications to NIAC. Primarily, the Council now reports to the President through the Secretary of Homeland Security.³⁷

³¹ (...continued)

Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. GAO-07-39. October 2006.

³² See *Federal Register*. Vol. 71 No. 57. pp. 14930-14933. March 24, 2006.

³³ See [http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm]. This site was last visited on January 15, 2008.

³⁴ White House Press Release, dated January 18, 2000.

³⁵ Executive Order 13231 — Critical Infrastructure Protection in the Information Age. *Federal Register*. Vol. 66. No. 202. October 18, 2001. pp. 53063-53071. The NIAC is established on page 53069.

³⁶ See White House Press Release, September 18, 2002.

³⁷ The current membership and activities of the National Infrastructure Advisory Council can be found on the DHS website. See [http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm]. Site was last visited on January 15, 2008.

Internal Agency Plans

There had been some confusion about which agencies were required by PDD-63 to submit critical infrastructure plans. The Directive required every agency to develop and implement such a plan. A subsequent Informational Seminar on PDD-63 held on October 13, 1998 identified two tiers of agencies. The first tier included lead agencies and other “primary” agencies like the Central Intelligence Agency and Veteran’s Affairs. These agencies were held to the Directive’s 180-day deadline. A second tier of agencies were identified by the National Coordinator and required to submit plans by the end of February 1999. The “secondary” agencies were Agriculture, Education, Housing and Urban Development, Labor, Interior, General Services Administration, National Aeronautics and Space Administration and the Nuclear Regulatory Commission. All of these “primary” and “secondary” agencies met their initial deadlines for submitting their internal plans for protecting their own critical infrastructures from attacks and for responding to intrusions. The Critical Infrastructure Assurance Office (CIAO) assembled an expert team to review the plans. The plans were assessed in 12 areas including schedule/milestone planning, resource requirements, and knowledge of existing authorities and guidance. The assessment team handed back the initial plans with comments. Agencies were given 90 days to respond to these comments. Of the 22 “primary” and “secondary” agencies that submitted plans, 16 modified and resubmitted them in response to first round comments.

Initially, the process of reviewing agency plans was to continue until all concerns were addressed. Over the summer of 1999, however, review efforts slowed and subsequent reviews were put on hold as the efficacy of the reviews was debated. Some within the CIAO felt that the plans were too general and lacked a clear understanding of what constituted a “critical asset” and the interdependencies of those assets. As a result of that internal debate, the CIAO redirected its resources to institute a new program called **Project Matrix**. Project Matrix is a three step process by which an agency can identify and assess its most critical assets, identify the dependencies of those assets on other systems, including those beyond the direct control of the agency, and prioritize. CIAO offered this analysis to agencies, including some not designated as “primary” or “secondary” agencies, such as the Social Security Administration and the Securities and Exchange Commission. Participation by the agencies was voluntary.³⁸

In the meantime, other agencies (i.e., those not designated as primary or secondary) apparently did not develop critical infrastructure plans. In a much later report by the President’s Council on Integrity and Efficiency (dated March 21, 2001), the Council, which was charged with reviewing agencies’ implementation of PDD-63, stated that there was a misunderstanding as to the applicability of PDD-63 to all agencies. The Council asserted that all agencies were required to develop a critical infrastructure plan and that many had not, because they felt they were not covered by the Directive. Also, the Council found that of the agency plans that had been submitted, many were incomplete, had not identified their mission-critical assets, and that almost none had completed vulnerability assessments. Two years later, the

³⁸ The use of Project Matrix’s methodology continues under HSPD-7.

Government Accountability Office³⁹ reported that four of the agencies they reviewed for the House Committee on Energy and Commerce (HHS, Energy, Commerce, and EPA) had still not yet identified their critical assets and operational dependencies, nor have they set any deadlines for doing so.⁴⁰

Interestingly, HSPD-7 reestablished a deadline for agencies to submit critical infrastructure protection plans to the Director of OMB for approval by July 2004. The Director of OMB provided guidance on how agencies should meet their requirement (Memorandum M-04-15, June 17, 2004). The memorandum stated that plans for the physical protection of assets would be subject to interagency review coordinated by the Department of Homeland Security, with DHS providing a written evaluation of each agency's plans within 120 days. Agency cyber security plans would be reviewed by OMB, as part of the requirements associated with the Federal Information Security Management Act of 2002, included as Title III of E-Government Act of 2002 (P.L. 107-347). These plans are to provide information to be included in the National Infrastructure Protection Plan (see below). DHS and OMB have not been willing to provide CRS with the status of these reports.

National Critical Infrastructure Plan

PDD-63 called for a National Infrastructure Assurance Plan that would be informed by sector-level plans and would include an assessment of minimal operating requirements, vulnerabilities, remediation plans, reconstitution plans, warning requirements, etc. The National Strategy for Homeland Security, and the Homeland Security Act each have called for the development of a comprehensive national infrastructure protection plan, as well, although without specifying deadlines and what that plan should include. HSPD-7 called for a comprehensive National Plan for Critical Infrastructure and Key Resources Protection by the end of 2004. According to HSPD-7, the National Plan should include (a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department will work with other stakeholders; (b) a summary of activities to be undertaken in order to carry out the strategy; (c) a summary of initiatives for sharing critical infrastructure information and threat warnings with other stakeholders; and (d) coordination with other federal emergency management activities.

In January 2000, the Clinton Administration released Version 1.0 of a *National Plan for Information Systems Protection*.⁴¹ In keeping with the original focus of PDD-63, the Plan focused primarily on cyber-related efforts within the federal government. The Bush Administration, through the President's Critical

³⁹ Note: The General Accounting Office has had its name changed legislatively to the Government Accountability Office.

⁴⁰ U.S. Government Accountability Office, Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors. Report to the Committee on Energy and Commerce, House of Representatives. GAO-03-233. February 2003. pp. 4-5.

⁴¹ *Defending America's Cyberspace. National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue.* The White House. 2000.

Infrastructure Protection Board, released *The National Strategy to Secure Cyberspace* in February 2003, which could be considered Version 2.0 of the Clinton-released Plan. It addressed all stakeholders in the nation's information infrastructure, from home users to the international community, and included input from the private sector, the academic community, and state and local governments. Also in February 2003, the Office of Homeland Security released *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. This strategy took a broad perspective of the issues and needs associated with organizing the nation's efforts to protect its critical infrastructure; identifying roles and responsibilities, actions that need to be taken, and guiding principles.

The Department of Homeland Security missed the December 2004 deadline for releasing the National Infrastructure Protection Plan called for in HSPD-7. It did publish an Interim National Infrastructure Protection Plan in February 2005. According to media reports, some in the private sector complained they were not adequately consulted.⁴² The Department subsequently released for public comment a "draft" National Infrastructure Protection Plan in November 2005.⁴³ A final version of the National Infrastructure Protection Plan (NIPP) was approved June 30, 2006.⁴⁴

The NIPP identifies and integrates specific processes by which an integrated national risk management effort can proceed. For example, it defines and seeks to standardize, across all sectors, the process for identifying and selecting assets for further analysis, identifying threats and conducting threat assessments, assessing vulnerabilities to those threats, analyzing consequences, determining risks, identifying potential risk mitigation activities, and prioritizing those activities based on cost-effectiveness.⁴⁵ The NIPP also calls for implementation plans for these risk reduction activities, with timelines and responsibilities identified, and tied to resources. Each lead agency is to work with its sector to generate **Sector Specific Plans**, utilizing the processes outlined in the NIPP. DHS will then use these same processes to integrate the sector specific plans into a national plan that identifies those assets and risk reduction plans that require national level attention because of the risk the incapacitation of those assets pose to the nation as a whole.

According to the NIPP, Sector Specific Plans (SSPs) were due 180 days after release of the NIPP (i.e. the end of 2006). Apparently, all 17 sectors met that

⁴² See "Still Waiting: Plan to Protect Critical Infrastructure Overdue from DHS," Congressional Quarterly. Homeland Security-Transportation & Infrastructure Newsletter, January 28, 2005. The Newsletter is electronic and available by subscription only. See [[@allnews&metapub=HSNEWS&seqNum=827&searchIndex=1](http://homeland.cq.com/hs/display.do?dockey=/cqonline/prod/data/docs/html/hsnews/109/hsnews109-000001507251.html)]. The article was last viewed on January 15, 2008.

⁴³ See *Federal Register*, vol. 70, no. 212, November 3, 2005, pp. 66840-66841.

⁴⁴ The NIPP can be found at [http://www.dhs.gov/xprevprot/programs/editorial_0827.shtml]. This site was last visited on January 15, 2008.

⁴⁵ For a discussion of a basic risk management process in a critical infrastructure context, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*, by John Moteff.

deadline. However, they went through a DHS review process before being released in May 2007. Of the 17 plans submitted, 7 were made available to the public, the rest were designated For Official Use Only.⁴⁶ The Government Accountability Office (GAO) reviewed 9 of the SSPs and found that while all complied, more or less, with the NIPP process, some plans were more developed and comprehensive than others.⁴⁷ As a result, GAO was unable to assess how far along each sector actually is in identifying assets, setting priorities, and protecting key assets. DHS views these SSPs as a first step in the process, and plans to review the sectors' annual progress reports, as required by HSPD-7. When or how these will be integrated into national plan is unclear.

It should be noted, that some sectors and agencies have performed already some or all of these risk management steps using various techniques and processes. The NIPP requires that each sector and lead agency ensure that previous work meets the basic requirements associated with the processes described in the NIPP.

Distinguishing between a strategy and plan, and whether these documents yet fulfill the requirement for the comprehensive national plan called for in the Homeland Security Act, is beyond the scope of this report. However, each succeeding document does appear to refine further some goal, objective, or initiative discussed in preceding documents.

Information Sharing and Analysis Center (ISAC)

PDD-63 envisaged a single ISAC to be the private sector counterpart to the FBI's National Infrastructure Protection Center (NIPC), collecting, analyzing, and sharing incident and response information among its members and facilitating information exchange between government and the private sector. The idea of a single ISAC evolved into each sector having its own center. ISACs differ somewhat from sector coordinating function in that they were to be 24/7/365 operations, where incidents experienced by owner/operators, as well as threat information from the government, could be reported, analyzed, and shared. Many were conceived originally as concentrating on cyber security issues, and some still function with that emphasis. However, others have incorporated physical security into their missions.

ISACs were formed around two primary models. One model involved ISAC members legally incorporating and establishing either their own ISAC operations or contracting operations out to a security firm. The banking, information, water, oil and gas, railroad, and mass transit sectors followed this approach.

The other model involved utilizing an existing industry or government-industry coordinating group and adding critical infrastructure protection to the mission of that group. The electric power (which uses North American Electricity Reliability

⁴⁶ See [http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtml#2] for a short discussion and to access those SSPs that are not designated as For Official Use Only. This site was last viewed on January 15, 2008.

⁴⁷ Government Accountability Office. *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*. GAO-07-706R. July 10, 2007.

Council (NERC)) and the telecommunications sector (which uses the National Coordinating Center (NCC)) followed this model. The emergency fire services sector incorporated ISAC functions into the existing operations of the U.S. Fire Administration, which has interacted with local fire departments for years.

Different federal financial support models were developed for ISACs, too. In some cases, ISACs received start up funding from their Lead Agency (e.g., drinking water received funding from EPA). In some cases, that support continues, in some cases the support has not continued (e.g., DOE no longer supports the energy ISAC). Other ISACs have always been self-supporting. The individual ISACs have formed a group called the ISAC Council.⁴⁸ Their formation and function experience some of the same variation as the coordinating councils, for some of the same reasons.

While PDD-63 envisioned ISACs to be a primary conduit for exchanging critical infrastructure information between the federal government and specific sectors, the Department of Homeland Security has developed a number of other information sharing systems and mechanism. For example, **US-CERT** (the U.S. Computer Emergency Readiness Team) publishes information on the latest computer-related vulnerabilities and threats and information on how to respond to a specific incident. U.S.-CERT also accepts incidents reports. It also manages the **National Cyber Alert System**, to which any organization or individual can subscribe. The Department also has developed a **Homeland Security Information Network (HSIN)**. HSIN initially served as the primary communication network for communicating and analyzing threat information between government law enforcement agencies at the federal, state, and local levels. The HSIN is being expanded to include each critical infrastructure sector (dubbed HSIN-CI) as part of the Critical Infrastructure Protection Partnership Model (i.e., through each sector and government coordinating council).

Shortly after September 11, 2001, the Department established what is now called the Infrastructure Protection **Executive Notification Service (ENS)**, which connects DHS directly with the Chief Executive Officers of major industrial firms. The ENS is used to alert partners to infrastructure incidents, to disseminate warning products, and to conduct teleconferences. The Department is also responsible for operating the **Critical Infrastructure Warning Network (CWIN)**, which provides secure communications between DHS and other federal, state, and local agencies, the private sector, and international agencies. CWIN does not rely on the Public Switch Network or the internet.

Identifying Critical Assets, Assessing Vulnerability and Risk, and Prioritizing Protective Measures

Among the activities assigned to the Information Analysis and Infrastructure Protection Directorate by the Homeland Security Act of 2002 were:

⁴⁸ See, [<http://www.isaccouncil.org/sites>]. This site was last visited on January 15, 2008.

- access, receive, analyze, and integrate information from a variety of sources in order to identify and assess the nature and scope of the terrorist threat;
- carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructure, of the United States including risk assessments to determine risks posed by particular types of attacks;
- integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures.

Furthermore, according to the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the Department of Homeland Security: (a) “in collaboration with other key stakeholders, will develop a uniform methodology for identifying facilities, systems, and functions with national-level criticality to help establish protection priorities;” (b) “will build a comprehensive database to catalog these critical facilities, systems, and functions;” and (c) “will also maintain a comprehensive, up-to-date assessment of vulnerabilities and preparedness across critical sectors.” Furthermore, these efforts “will help guide near-term protective actions and provide a basis for long-term leadership focus and informed resource investment.”

Following September 11, 2001, owners/operators of critical infrastructure assets, to varying degrees, began identifying critical assets, assessing their vulnerabilities to attack, and developed security plans or beefed up protections. For example, the Federal Transit Authority assessed the vulnerabilities of the nation’s largest mass transit systems. The freight rail companies developed additional security measures to coincide with the level of threat identified by DHS’s color-coded National Alert System. Drinking water authorities, through the Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188), were required to conduct vulnerability assessments and to develop security plans based on those assessments. Port facilities and maritime vessels were required by the Maritime Transportation Security Act (P.L. 107-295) to do the same. The American Petroleum Institute, the North American Electric Reliability Council, and other industry associations offered guidance to their respective members on how to conduct vulnerability assessments and to manage their risk from possible attack. However, DHS’s ability to coordinate this activity developed more slowly, and its ability to develop a uniform methodology that would allow it to generate a set of national priorities is unfolding just now with the release of its NIPP, described above.

However, during this same time, DHS has engaged in at least two other sets of activities that have, also to varying degrees, identified critical assets, assessed their vulnerabilities, and provided assistance to increase protection of these sites.

Shortly before the beginning of Operation Iraqi Freedom in 2003, as part of Operation Liberty Shield⁴⁹, what was then called the Protective Services Division of

⁴⁹ Operation Liberty Shield was a comprehensive national plan to protect the homeland
(continued...)

the newly-formed Information Analysis and Infrastructure Protection Directorate, identified a list of 160 assets or sites, including chemical and hazardous materials sites, nuclear power plants, energy facilities, business and finance centers, and more, that it considered critical to the nation based on their vulnerability to attack and potential consequences. During the course of the year, that list grew to 1,849 assets or sites.⁵⁰

According to testimony before the House Appropriations Committee on April 1, 2004, then-Undersecretary for Information Analysis and Infrastructure Protection, Frank Libutti, made reference to 1700 sites identified by DHS as being high priority sites.⁵¹ According to the testimony, DHS intended to visit each of these sites to assess their vulnerabilities to various forms of attack and to meet with local law enforcement officials to assist them in developing **Buffer Zone Protection Plans (BZPPs)**. BZPPs focus on protections that can be taken “outside the fence,” including how to identify threatening surveillance, patrolling techniques, and how to assert command and control if an incident should occur. DHS has provided training and technical assistance to help state and local law enforcement entities develop their own BZPPs. The BZPP activity is now integrated into the State and Local Grants Program. In addition to these “outside the fence” activities, DHS has conducted **Site Assistance Visits (SAVs)** at selected sites, on a voluntary basis, to discuss with owners and operators vulnerabilities and protective measures that can be taken “inside the fence.” SAVs form an integral part of the “**comprehensive reviews (CRs)**” which DHS is performing on both nuclear power facilities and high-priority chemical facilities. Once these two sectors are completed, DHS is planning to conduct comprehensive reviews of other sectors.

In addition to its selection of high priority sites and subsequent site visits, vulnerability assessments, and buffer zone protection plans, DHS, through its Office of Grants and Training, also has been supporting infrastructure protection at the state and local level through its State and Local Grant Programs. Specific grant programs include the State Homeland Security Formula-based Grants, the Urban Area Security Initiative (UASI) Grants (both of which primarily support first responder needs, but include certain infrastructure protection expenditures), Port Security Grants, Rail and Transit Security Grants, Intercity Bus Security Grants, and Highway Security Grants. The Buffer Zone Protection Plan grants have been added to this set of programs. Before receiving funds, grants recipients must identify specific critical infrastructure assets, conduct threat and vulnerabilities assessments, and develop a plan for how they intend to use grant funds to reduce those vulnerabilities through eligible expenditures.⁵²

⁴⁹ (...continued)
during operations in Iraq.

⁵⁰ See, Department of Homeland Security, Office of the Inspector General. *Progress in Developing the National Asset Database*. OIG-06-04. June 2006.

⁵¹ According to the Department’s Inspector General report, these 1,700 assets refer to the 1,849 assets identified in its research.

⁵² For more information on the grant programs and the FY2007 awards, see CRS Report (continued...)

Issues and Discussion

Congressional interest in critical infrastructure protection is focused, principally, on reviewing the progress and effectiveness of DHS's efforts.

Identifying Critical Assets, Functions, and Systems

There has been some debate about the progress and effectiveness of DHS's efforts at identifying high priority assets. For example, when developing the initial list of priority sites during Operation Liberty Shield, certain utility operators, when presented a list of what DHS considered to be critical electric power assets, noticed that some of the entries were not currently in use.⁵³ According to the DHS Inspector General, DHS itself determined that its early list of priority sites was unreliable.⁵⁴

Over time, according to the DHS Inspector General, this initial priority list evolved into what is now called the **National Asset Database**, which, as of January 2006, contained over 77,000 entries. While DHS apparently has made progress on the reliability of the information contained in the Database, it continues to draw criticism for including thousands of assets that many believe have more local importance than national importance. There is some confusion as to what the National Asset Database is meant to be. Critics of the Database assume it is a continuation of DHS's list of high priority sites. DHS asserts that it is an inventory of assets, from which critical assets may be drawn.⁵⁵

In his response to the Inspector General's report, the Undersecretary for Preparedness stated that DHS does not intend to have one definitive prioritized list of critical assets. He further stated that it would not be possible or useful to develop one.⁵⁶ However, the Assistant Secretary for Infrastructure Protections has stated that DHS does maintain a list of roughly 600 high priority sites, which it uses to focus DHS operations, resource allocation and grants.⁵⁷ It is not clear from these officials'

⁵² (...continued)

RL33583, *Homeland Security Grants: Evolution of Program Guidance and Grant Allocation Methods*; and CRS Report RS22383, *FY2007 Appropriations for State and Local Homeland Security*, both by Shawn Reese.

⁵³ Based on personal communication with industry official, September 29, 2003.

⁵⁴ Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database*. Op. cit., p. 16.

⁵⁵ For more discussion of the issues associated with the National Asset Database see, CRS Report RL33648, *Critical Infrastructure: The National Asset Database*, by John Motteff.

⁵⁶ Department of Homeland Security. Office of the Inspector General. *Progress in Developing the National Asset Database*. Op. cit., p. 31.

⁵⁷ *USA Today*. "Database is Just the 1st Step," by Robert Stephan. July 21, 2006. p. 8A. In testimony before the Senate Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, Senate Committee on Homeland Security and Governmental Affairs, July 12, 2007, the Assistant Secretary stated that this list has grown to about 2,500
(continued...)

statements what relation this current list of approximately 600 high priority sites has to DHS's earlier priority list or the current Database.

Also, implementation of the National Infrastructure Protection Plan (NIPP) is suppose to contribute to the identification of assets that are most critical to the nation. It remains to be seen how effective this process will be.

Assessing Vulnerabilities and Risk

Assuming DHS does maintain a list of high priority assets, it is not clear how many of these have been visited, had their vulnerability and risk assessed, or have had buffer zone protection plans or other protective measures developed and implemented to-date. Directorate budget requests report some figures, but the reporting is not consistent nor standardized from year to year. Also, reference to high-priority sites in earlier years may not refer to the same list of high-priority sites currently under consideration.

According to the Directorate's FY2006 budget request, between 150 and 180 SAVs had been conducted during FY2004. According to its FY2007 budget request, 200 were conducted in FY2005, and another 150 were expected to be conducted per year after that. The FY2008 budget request is silent on how many SAVs were conducted subsequent to FY2005.

According to the Senate Appropriation Committee's report accompanying the FY2005 DHS appropriation,⁵⁸ 150 vulnerability assessments of high valued sites were expected to be completed in FY2004, and another 400 to be assessed in FY2005. According to the IA/IP FY2006 budget request, vulnerability assessments had been conducted at 50 high-priority sites during FY2004. The FY2007 budget request is silent on how many vulnerability assessment were completed in FY2005. The FY2008 budget request stated that vulnerability assessments had been conducted at 66 high-priority sites in FY2006, presumably in addition to those conducted in prior years.

According to the IA/IP FY2006 budget request, 800 BZPP's had been implemented by the end of the calender year 2004. The FY2006 budget request also stated that the Directorate planned to ensure that 1000 BZPPs would be implemented in FY2005. The FY2007 budget request stated that BZPPs had been implemented at over 1800 high priority sites in FY2005. The FY2008 budget request stated that BZPP's for 1620 sites were submitted (presumably to the Office of Grants and Training) and approved for grants in FY2006. The number of sites for which BZPPs have been prepared or approved exceed the roughly 600 sites currently considered high-priority by the Directorate. Now that the BZPP program has been integrated with the other state and local grant programs, the 1600 to 1800 sites referred to above may include sites not necessarily considered high-priority by the Directorate.

⁵⁷ (...continued)

assets.

⁵⁸ U.S. Congress. Senate. *Department of Homeland Security Appropriations Bill, 2005*. Report accompanying S. 2537. S.Rept. 108-280. June 17, 2004. p. 77.

DHS's Performance Budget Overview for FY2008 for the Directorate presents a different perspective on the number of site visits, vulnerability assessments and BZPPs that have been, or will be, completed and implemented at high priority sites by the end of FY2008. DHS's Performance Budget Overview matches specific programs with specific performance measures. The Infrastructure Protection and Risk Management Program (referred to in the FY2007 Performance Budget Overview as the Infrastructure Protection Program and apparently referring to the non-cyber and non-communications related activities of the Infrastructure Protection and Information Security Program in the budget) has three performance measures listed: the percentage of high priority sites at which BZPP's have been implemented; the percentage of high-priority sites for which vulnerability assessments have been conducted and corresponding resource allocations made; and the percentage of high-priority sites at which at least two protective measures have been implemented. The targets and actual percentages for each of these measures are listed in the Table below. According to this performance based budget review, 15% of high-priority sites have had vulnerability assessments. Note, there is a two year lag in the availability of actual data.

Table 3. Performance Measures for the Infrastructure Protection and Risk Management Program

Measure		FY2005	FY2006	FY2007	FY2008
Pct. of high-priority [sites] for which a BZPP has been implemented	target	70%	28%	65%	70%
	actual	18%	58%	N/A	N/A
Pct. of high-priority [sites] at which a vulnerability assessment has been conducted, and make corresponding resource allocation decisions	target	10%	15%	25%	30%
	actual	14%	15%	N/A	N/A
Pct. of high-priority [sites] at which at least two protective measures have been implemented	target	None	10%	20%	25%
	actual	None	14%	N/A	N/A

Source: Department of Homeland Security, National Protection and Programs Directorate, FY2008, Strategic Context, Congressional Justification, 2007.

Allocating Resources

It is a matter of policy, as articulated in the documents discussed above, that federal resources should focus on those critical infrastructure assets that, if attacked, pose the greatest risks to the nation.

Risk, in the context of critical infrastructure and terrorism, can be defined as the potential consequence associated with a particular kind of attack or event against a particular target, discounted by the likelihood that such an attack or event will occur

(threat) and the likelihood that the target will sustain a certain degree of damage (vulnerability). Threat includes not only the identification of specific adversaries, but also their intentions and capabilities (both current and future). Consequences include lives and property lost, short term financial costs, longer term economic costs, environmental costs, etc. Given this definition, risk is not threat, nor vulnerability to a threat, nor the estimated consequences associated with a specific attack, but some integration of the three.⁵⁹

According to the NIPP, the allocation of resources is to be a two step process. First, those critical assets which pose the greatest risk to the nation if attacked (i.e., those assets that score highest when integrating threat, vulnerability, and consequences) are to be given the highest priority. The second step is to identify and support those protective measures that are likely to provide the greatest risk reduction for any given investment.

Federal resources are spent in a number of ways, including agencies' internal budgets for operations and programs, grants to states and localities, and research and development funding for universities and industry. The most publicized debates on the allocation of federal resources focuses primarily on grants to states and localities. The formula-based State Homeland Security Grants, mentioned above, has been criticized by some for allocating more dollars per capita to states that some perceive as having lower risks than other states. Congress has been at odds on if, or how, to modify the allocation of those funds. The other grant programs mentioned above (i.e., Urban Area Security Initiative grants and the sector specific grants) are discretionary. According to DHS, allocation of these funds are based on a calculation not only of risk, but also on need. With the allocation of FY2006 Urban Area Security Initiative grants, some cities which perceive themselves as having greater risk (or at least being more at threat or could suffer greater losses) received less funding than they did the previous year, while other cities perceived as having lower risks saw their funds increased. DHS stated that one reason for this was the way it determined the unmet needs of the area and the programs proposed by the areas to address those needs. Faced with criticism from those cities and states that received a drop in funds, DHS stated it would rework its grant review process. In addition, Congress has requested that the Government Accountability Office review the validity, relevance, reliability, timeliness and availability of the risk factors used by DHS in its discretionary grant programs.⁶⁰ Meanwhile, Congress continues to set its own priorities by specifying the amount of funds that go to each of these grants programs.

⁵⁹ Note, that in many cases these factors may not be independent. In other words, the likelihood that a particular asset may be attacked may increase if it is perceived to have a high vulnerability and/or the consequences of the attack are great. For more discussion of how risks can be assessed and its implications for decision making, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*, by John Motteff.

⁶⁰ For a detailed discussion of the risk assessment process used to allocate grant funds to urban areas, see CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins.

Also, it is not clear to what extent the NIPP process influences the allocation of resources to states and localities. DHS states that information contained in the National Asset Database is reviewed in making these grant allocation decisions. However, these grant programs are managed by the Office of Grants and Training, which apparently assesses risks independent of the NIPP. Similarly, port security grants, while managed by the Office of Grants and Training, are influenced largely by the review of vulnerability assessments and security plans performed by the Coast Guard.

Information Sharing

Information sharing in the context of homeland security encompasses a very complex network of proposed connections. There is information sharing between federal agencies, especially between intelligence agencies, and between intelligence and law enforcement agencies. There is information sharing between federal agencies and their state and local counterparts. There is information sharing between federal, state, and local agencies and the private sector. There is information sharing within and between the private sectors. And there is information sharing between all of these entities and the public. A multitude of mechanisms have been established to facilitate all of this information sharing. While the multitude of mechanism may cause some concern about inefficiencies, a highly connected, in some cases redundant, network may not be a bad thing. A primary concern is if these mechanisms are being used and are effective.

In the past, information flow between all of these stakeholders has been restrained, or non-existent, for at least three reasons: a natural bureaucratic reluctance to share information, technological difficulties associated with compatibility, and legal restraints to prevent the misuse of information for unintended purposes. However, in the wake of September 11, given the apparent lack of information sharing that was exposed in reviewing events leading up to that day, many of these restraints are being reexamined and there appears to be a general consensus to change them. Some changes have resulted from the USA PATRIOT Act (including easing the restrictions on sharing of information between national law enforcement agencies and those agencies tasked with gaining intelligence of foreign agents). The legislation establishing the Department of Homeland Security also authorizes efforts to improve the ability of agencies within the federal government to share information between themselves and other entities at the state and local level. The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) reorganized the entire intelligence community, in part to improve the level of communication and coordination between the various intelligence organizations.⁶¹ The legislation also required the President to establish an **information sharing environment (ISE)** for the sharing of terrorism information among all appropriate federal, state, local, and tribal entities, and the private sector.

While the federal government is trying to increase the amount of information shared among appropriate stakeholders, it is also trying to maintain a tight control

⁶¹ See also CRS Report RL32366, *Terrorist Identification, Screening, Tracking Under Homeland Security Presidential Directive 6*, by William J. Krouse.

(short of classification) on who gets to see what information. A variety of designations have been given to information the federal government wishes to control (critical infrastructure information (see below), homeland security information, terrorism information, sensitive security information). A catch-all term for these and other designations of controlled information is “**sensitive but unclassified**.”

Since much of what is considered to be critical infrastructure is owned and operated by the private sector, critical infrastructure protection relies to a large extent on the ability of the private sector and the federal government to share information. However, it is unclear how open the private sector and the government have been in sharing information. The private sector primarily wants from government information on specific threats which the government may want to protect in order not to compromise sources or investigations. In fact, much of the threat assessment done by the federal government is considered classified. For its part, the government wants specific information on vulnerabilities and incidents which companies may want to protect to prevent adverse publicity or to keep confidential company practices. The private sector, too, is concerned about whether providing this information might lead to future regulatory action or other liabilities. Successful information sharing will depend on the ability of each side to demonstrate it can hold in confidence the information exchanged.

Sharing information between government and the private sector is made more complex by the question of how the information will be handled within the context of the Freedom of Information Act (FOIA). In particular, the private sector is reluctant to share the kind of information the government wants without it being exempt from public disclosure under the existing FOIA statute. The Homeland Security Act (P.L. 107-296, Sec. 214) exempts information defined as **critical infrastructure information** from FOIA (as well as providing other protections). Similar FOIA exemptions are offered in other legislation. For example, the Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188, Sec. 401, see below) exempts certain security-related information from FOIA. Even with these protections in statute, it is uncertain how much information on assets, vulnerabilities, incidents, etc. is being shared with DHS, or how useful it is.⁶²

The FOIA exemptions for critical infrastructure information (CII) and other types of sensitive but unclassified information is not without its critics. The non-government-organizations that actively oppose government secrecy are reluctant to expand the government’s ability to hold more information as classified or sensitive. These critics, and others, feel that the protections offered to CII and other types of sensitive but unclassified information is too broad and believe that controls are

⁶² In February 2005, DHS acknowledged the receipt of 29 submissions of CII documents, 22 of which were approved as CII by DHS. See *DHS Finally Speaks on CII* at [<http://www.ombwatch.org/article/articleprint/2683-1/321>]. Site last viewed on January 15, 2008. In previously cited testimony (before the Senate Ad Hoc Subcommittee on State, Local, and Private Sector Preparedness and Integration, July 12, 2007), the Assistant Secretary for Infrastructure Protection stated that since the final rule governing implementation of the CII program was released, DHS has received about 5,400 submissions.

stifling public debate and oversight, as well as impeding technological advances that could benefit both security and the economy.⁶³

Regulation

As a general statement of policy, owners and operators of critical infrastructure are to work with the federal government on a voluntary basis. Sharing information with the federal government about vulnerability assessments, risk assessments, and the taking of additional protective actions is meant to be voluntary.

However, the degree to which some of the activities are mandated varies across sectors. In some cases, sectors are quite regulated. Nuclear power plants must meet very specific standards for assessing their vulnerabilities to very specific types of attacks and to take the necessary actions to address those vulnerabilities. The Nuclear Regulatory Commission enforces these regulations. The Maritime Transportation Security Act (P.L. 107-295) requires facilities at ports, and certain vessels, to conduct vulnerability assessments and to develop and implement security plans (including naming a security officer who is responsible for developing and implementing these plans). The vulnerability assessments and security plans are reviewed by the Coast Guard. The Public Health Security and Bioterrorism Preparedness Act (P.L. 107-188) requires community drinking water systems to conduct vulnerability assessments and to incorporate the results of those assessments into their emergency response plans. The vulnerability assessments must be submitted to the Environmental Protection Agency (EPA). The EPA must also receive certification that the emergency response plans have been appropriately modified to reflect the vulnerability assessments. This same Act also amended the Federal Food, Drug, and Cosmetic Act to require all facilities engaged in manufacturing, processing, packing, or holding food for consumption to register with the Department of Health and Human Services. In addition, the Food and Drug Act was amended to require regulations specifying the types of information these facilities needed to keep on record for a specified amount of time to assist the Secretary in determining if a food product has been adulterated and represents a public health problem. The FY2006 DHS appropriation bill (P.L. 109-295, Sec. 550), authorized the Secretary of Homeland Security to issue interim final regulations requiring vulnerability assessments and security plans for certain chemical facilities, except those covered by the Maritime Transportation and Security Act, other relevant acts affecting drinking water authorities, or those operated by the Department of Energy, the Department of Defense, or the Nuclear Regulatory Commission.

At the other end of the spectrum are sectors such as information and telecommunication, oil and gas, and commercial (i.e., malls and office buildings) where similar activities (i.e., vulnerability assessments, etc.) are encouraged but not mandated.

⁶³ For a discussion of sensitive but unclassified information — not only science and technology information, but other types of information held by, or given to, the federal government — see CRS Report RL33303, “*Sensitive But Unclassified Information*” and *Other Controls: Policy and Options for Scientific and Technical Information*, by Genevieve J. Knezo.

Appendix

Federal Funding for Critical Infrastructure Protection

It is not possible to determine definitively how much funding the federal government devotes to critical infrastructure protection. The Homeland Security Act requires the President's Budget to include a budget analysis of homeland security activities across the federal government. For purposes of its analysis, OMB categorizes funding according to the mission areas defined in the *National Strategy for Homeland Security*. These include intelligence and warning; border and transportation security; domestic counter-terrorism; critical infrastructure and key asset protection; defending against catastrophic events; and emergency preparedness and response. While there is a separate category for critical infrastructure protection, activities included in some of the other mission areas can also be relevant or necessary for critical infrastructure protection. Table A.1. below shows the funding figures for the critical infrastructure protection mission area taken from the FY2008 budget's analysis.

Table A.1. Critical Infrastructure Protection Funding by Department
(\$ in millions)

Department	FY2006 actual	FY2006 suppl.	FY2007 enacted/ CR ^a	FY2007 suppl.	FY2008 request
Agriculture	90.7		31.1		64.0
Defense	11150.5	862.3	11254.0		11966.2
Energy	1520.6		1515.1		1607.1
HHS	181.7		184.8		180.2
Homeland Security	2698.3		2779.6		3035.5
Justice	541.1		531.2	3.0	494.3
Transportation	131.9		131.9		166.1
Veterans Affairs	262.5		208.3		221.9
NASA	212.6		199.2		193.9
NSF	317.2		317.2		350.4
Social Security	174.6		191.9		215.0
Other Agencies	651.7	0.1	575.4		601.6
Grand Total	17933.2	862.4	17919.7	3.0	19096.1

Source: OMB, Budget of the U.S. Government, FY2008Analytical Perspectives. Chapter 3. Homeland Security Funding Analysis. p. 26.

a. Except for DOD and DHS, figures for FY2007 are based on the full year estimate of then-operative continuing resolution (CR). Actual figures will differ according to the final allocation of funds appropriated through the Continuing Appropriations Resolution, 2007 (P.L. 110-5).

Much of this funding is spent by agencies to protect their own critical infrastructure. It also includes funds that agencies may spend working with states, local governments, and private owners/operators to reduce their respective vulnerabilities. DHS activities include both of these, as well as activities associated with coordinating the national effort.

Other mission areas include activities that might also be considered part of the effort to protect critical infrastructure. For instance, the intelligence and warning mission area includes threat analysis, risk analysis, and the sharing of that information with other stakeholders, including states, localities, and the private sector, each of which factor into critical infrastructure protection. Border and transportation security includes activities associated with protecting airports, sea ports, and other transportation modes.

In many cases, funding for homeland security (and critical infrastructure protection) is buried within a number of different accounts, activities, programs, and projects. It is not possible to track Congressional appropriations in each of these mission areas within the agencies' appropriations bills. Agencies may not know themselves until their appropriations are allocated. Also, in the Table above, the FY2007 figures, except those for Homeland Security and Defense (which had appropriations passed by the 109th Congress), are based on funding provided by the then-operative continuing resolution. Actual funding for FY2007 will differ according to the final allocation of funds appropriated through the Continuing Appropriations Resolution, 2007 (P.L. 110-5).

The National Protection and Programs Directorate's FY2008 Budget Request and Appropriations for Infrastructure Protection and Information Security and Other Relevant DHS Budget Activities

Just as it is difficult to account for all the federal activities associated with critical infrastructure protection in the federal government, it is also difficult to track the critical infrastructure protection activities within the Department of Homeland Security. Funding for activities related to critical infrastructure protection is found in numerous places within the Department, including the National Protection and Programs Directorate, the Transportation Security Administration, the Coast Guard, Secret Service, the Science and Technology Directorate, Office of Grants and Training, and U.S. Customs and Border Protection. Much of the funding for the organizations and activities discussed in the body of this report can be found in the Infrastructure Protection and Information Security (IPIS) Program. Below (**Table A.2**), is the FY2008 budget request and appropriations for the IPIS program within the National Protection and Programs Directorate's budget.⁶⁴

⁶⁴ The IPIS budget activity supports many of the same (though slightly restructured) infrastructure protection activities that have evolved from the days of the “old” Information Analysis and Infrastructure Protection Directorate.

Table A.2 Funding for the Infrastructure Protection and Information Security Program
(\$ in millions)

Infrastructure Protection and Information Security Budget Activity						
Program/Project Activity	FY2006 actual	FY2007 enacted	FY2008 Request	FY2008 House Apprн.	FY2008 Senate Apprн.	Final FY2008 Apprн. Enact'd
Management and administration	81,400	77,000	—	—	—	
Critical infrastructure outreach and partnerships	110,200	101,100	—	—	—	
Critical infrastructure identification and evaluation	45,735	69,000	—	—	—	
National infrastructure simulation and analysis center	19,800	25,000	—	—	—	
Biosurveillance	11,649	8,218	—	—	—	
Protective actions	87,559	32,043	—	—	—	
Infrastructure Protection	—	—	240,116	271,584	252,110	272,596
Cyber security	85,108	92,000	97,688	87,073	92,000	210,413
National security/emergency preparedness telecommunications	135,853	143,272	164,773	128,524	137,074	136,021
Office of Emergency Communications	—	—	35,700	45,700	45,915	35,700
Total IPIS	577,304	547,633	538,277	532,881	527,099	654,730

Source: FY2008 Congressional Justification. National Protection and Programs Directorate. Overview. Budget Justification. February 2007. Department of Homeland Security Appropriations Bill 2008, H.Rept. 110-181 (accompanying H.R. 2638) and S.Rept. 110-84 (accompanying S. 1644). The Consolidated Appropriations Act, 2008 (H.R. 2764, P.L. 110-161); see Congressional Record, December 17, 2007, Part II, H16092.

In the past, the IPIS budget supported eight program or project activities (PPAs). In the FY2008 budget request, those activities not specifically focused on cyber security and telecommunications activities were consolidated into a single Infrastructure Protection PPA. Table A.2 compares the old IPIS PPA structure with

the new PPA structure. However, the FY2006 and FY2007 figures cannot be compared directly with the FY2008 figures. The NPPD FY2008 budget request realigned some expenses that do not allow a direct comparison. For example, the FY2008 budget request transferred expenses, such as rents and related facility costs, and information technology support, which had previously been charged to individual IPIS PPAs, to the Directorate's Management and Administration budget activity (not to be confused with the "old" IPIS Management and Administration PPA listed in the Table). The FY2008 budget request also distributed salaries and related expenses to each of the IPIS PPAs. In FY2006 and FY2007, all IPIS-related salaries and expenses were part of the IPIS Management and Administration PPA. Other changes include the transfer of the Biosurveillance PPA to the Office of Health Affairs (part of the Secretary's consolidation of bio-defense activities) and the addition of activities associated with the Office of Emergency Communications (directed by the Post-Katrina Act).

While consolidating a number of PPAs into a single Infrastructure Protection (IP) PPA in its FY2008 budget request, the Directorate did provide a structure by which to categorize the specific programs and activities being conducted under the IP PPA. The specific programs and activities were divided into three areas: Identification and Analysis, Coordination and Information Sharing, and Risk Reduction Activities. The budget justification document did not provide a further breakdown of IP funding to this level. However, DHS apparently provided these figures to the appropriations committees during the development of the appropriation bills, and Congress did specify funding for each of the three funding categories, apparently renaming Risk Reduction Activities to Mitigation Programs, and adding a fourth category (Risk Analysis). This latter category was dropped in the Consolidated Appropriations Act. Congress ended up appropriating approximately \$30 billion more for the IP PPA than was requested. Based on the requested budgets for these categories reported by the committees, Congress directed most of the increase to Mitigation Programs.

As noted in the table above, Congress provided a sizable increase for Cyber Security within the IPIS budget. The increase in the Cyber Security PPA primarily supports an amended budget request submitted by the Administration in November 2007. The amended request added \$115 million to the original Cyber Security request for programs to enhance the cyber security of federal civilian networks.

In addition to the IPIS program within the National Protection and Programs Directorate, other areas in DHS support infrastructure protection. A major component of support for critical infrastructure protection within the Department are the State Homeland Security Grants, the Urban Area Security Initiative Grants, and the Transportation and Infrastructure Protection Grants (which include ports, rail, trucking, mass transit, and intercity bus), all administered by the Office of Grants, relocated with the Federal Emergency Management Agency (FEMA). The State Homeland Security Grants and the Urban Areas Security Initiative Grants primarily support first responder capabilities, but funding can also be spent on critical infrastructure protection expenses (such as the purchase of cameras, sensors, etc.). For FY2008, the Administration requested \$250 million for State Homeland Security Grants, \$800 million for the Urban Area Security Initiative, and \$456 million in Transportation and Infrastructure Grants. For more information on these grants, see

CRS Report RS22596, *FY2008 Appropriations for State and Federal Homeland Security*.

The Transportation Security Administration (TSA) is responsible for overseeing the security of the nation's transportation sectors (as directed by the Aviation and Transportation Security Act, P.L. 107-71). Aviation security consumes a large fraction of the TSA budget. The Administration requested \$4.9 billion in FY2008 for all facets of aviation security activities such as passenger and baggage screening; the purchase, installation, and operation of explosive detection equipment; and airport perimeter security. TSA also receives funds for surface transportation security and security-related support activities.

Also, the Science and Technology Directorate budget supports research and development in a number of areas relevant to critical infrastructure protection. This includes research and development in cyber security, risk analysis, explosive detection, blast protection, modeling and simulation, safe cargo containers, defense against man-portable air defense systems (MANPADS), and more. The Directorate also works with the Office of Infrastructure Protection to develop and maintain a National Critical Infrastructure Protection R&D Plan. It is difficult to determine how much funding is devoted overall to critical infrastructure protection-related research, given the budget structure of the programs.

To track the funding for these programs, the reader should see CRS Report RL34004, *Homeland Security Department: FY2008 Appropriations*, coordinated by Jennifer E. Lake and Blas Nuñez-Neto.